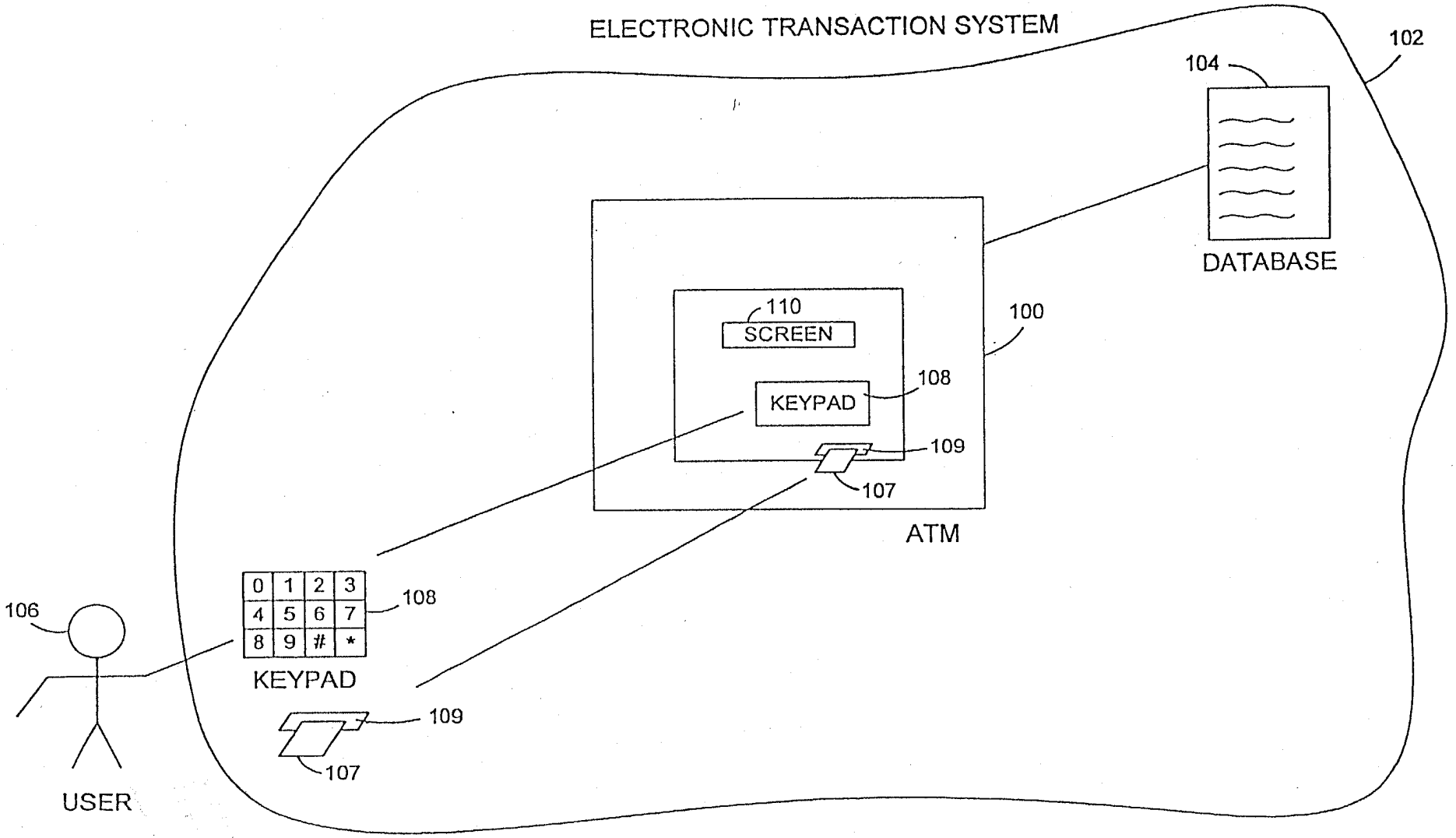



FIG. 1 (PRIOR ART)

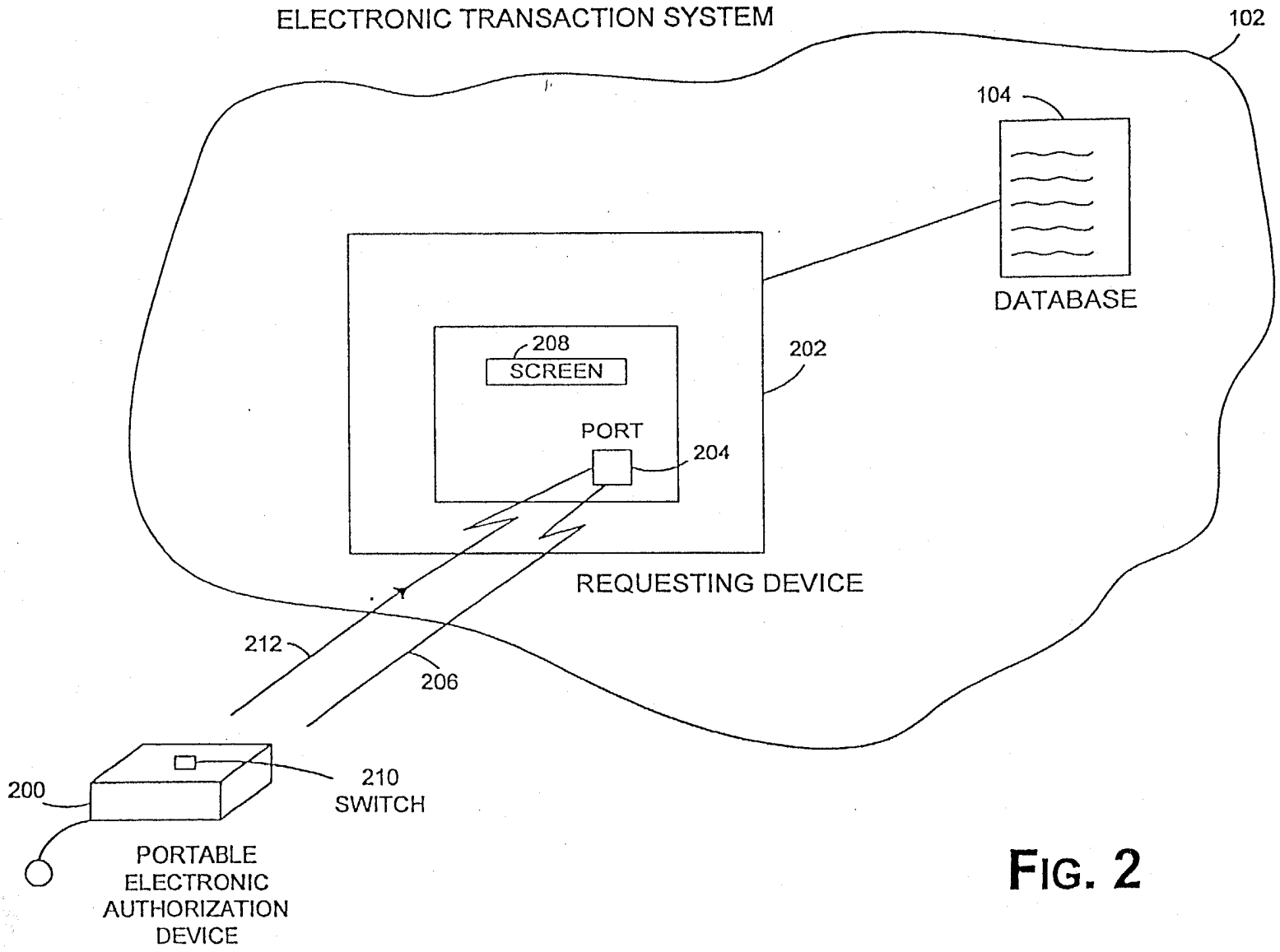

ELECTRONIC TRANSACTION SYSTEM
102
104
DATABASE
208
SCREEN
202
PORT
204
REQUESTING DEVICE
212
206
200
210
SWITCH
PORTABLE
ELECTRONIC
AUTHORIZATION
DEVICE

FIG. 2

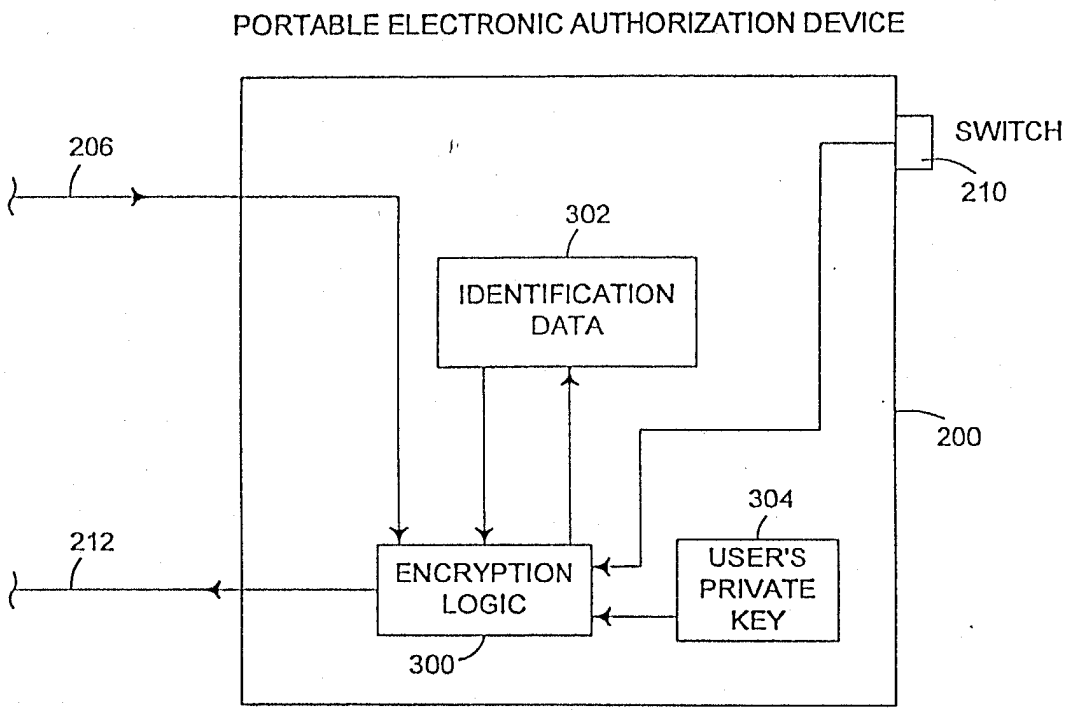

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
206
SWITCH
210
302
IDENTIFICATION DATA
200
304
212
ENCRYPTION LOGIC
USER'S PRIVATE KEY
300

FIG. 3A

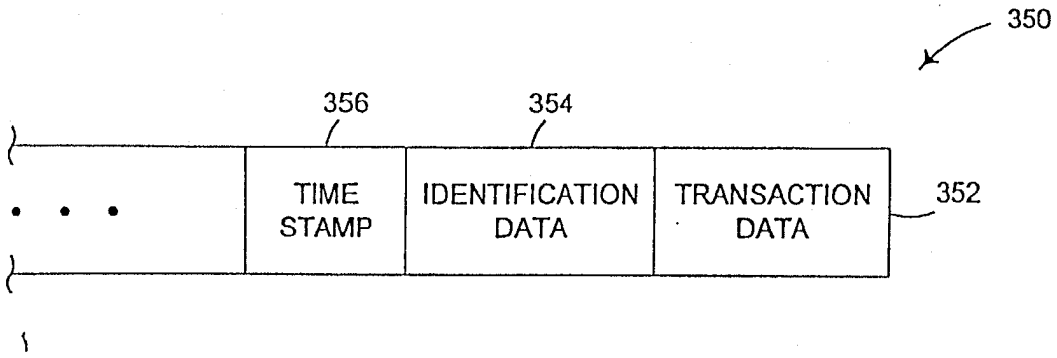

350
356
354
TIME STAMP
IDENTIFICATION DATA
TRANSACTION DATA
352

FIG. 3B

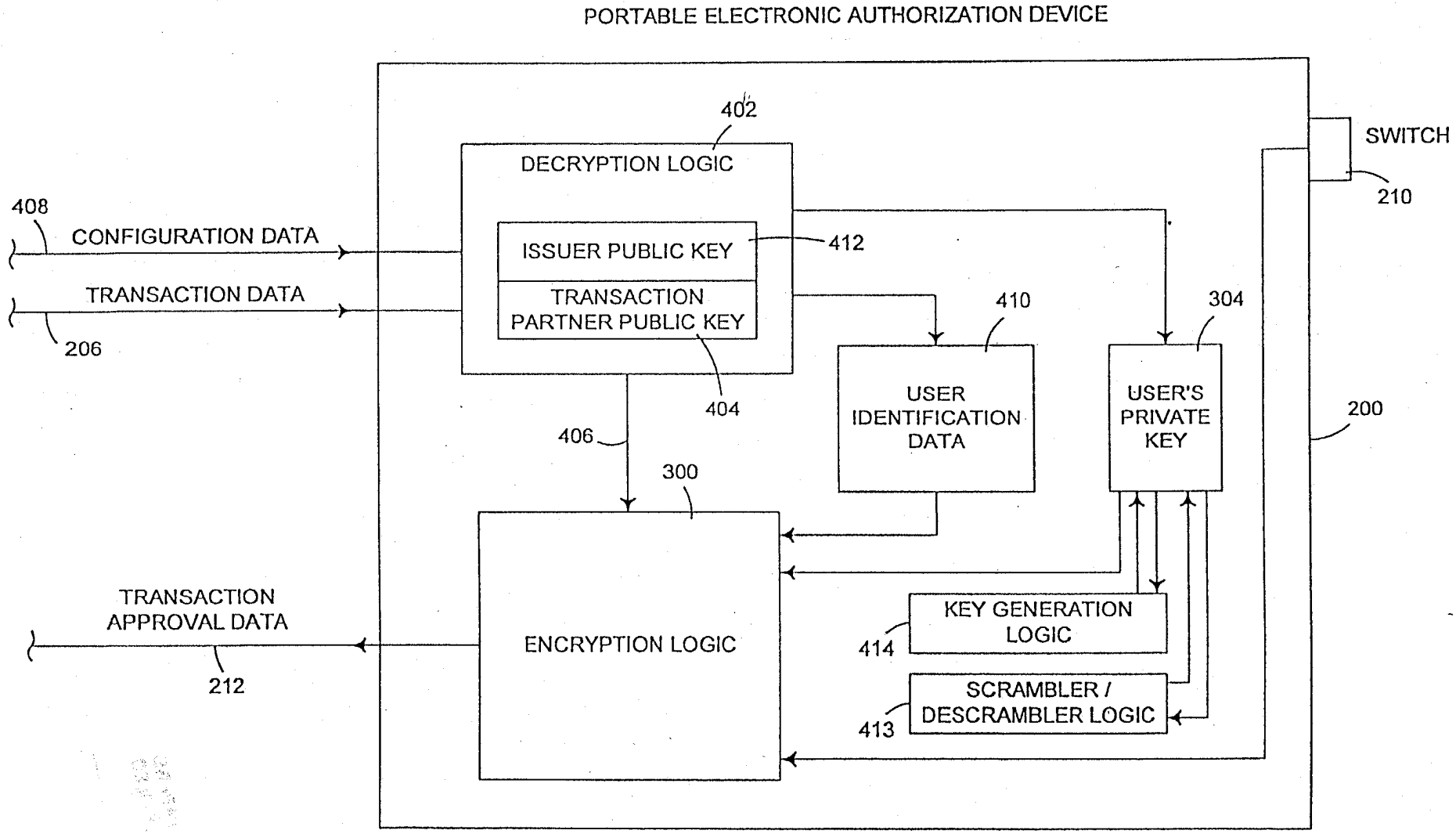

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
402
DECRYPTION LOGIC
SWITCH
210
408
CONFIGURATION DATA
ISSUER PUBLIC KEY
412
TRANSACTION DATA
TRANSACTION PARTNER PUBLIC KEY
206
404
410
304
USER IDENTIFICATION DATA
USER'S PRIVATE KEY
200
406
300
TRANSACTION APPROVAL DATA
ENCRYPTION LOGIC
KEY GENERATION LOGIC
414
SCRAMBLER / DESCRAMBLER LOGIC
413
212

FIG. 4

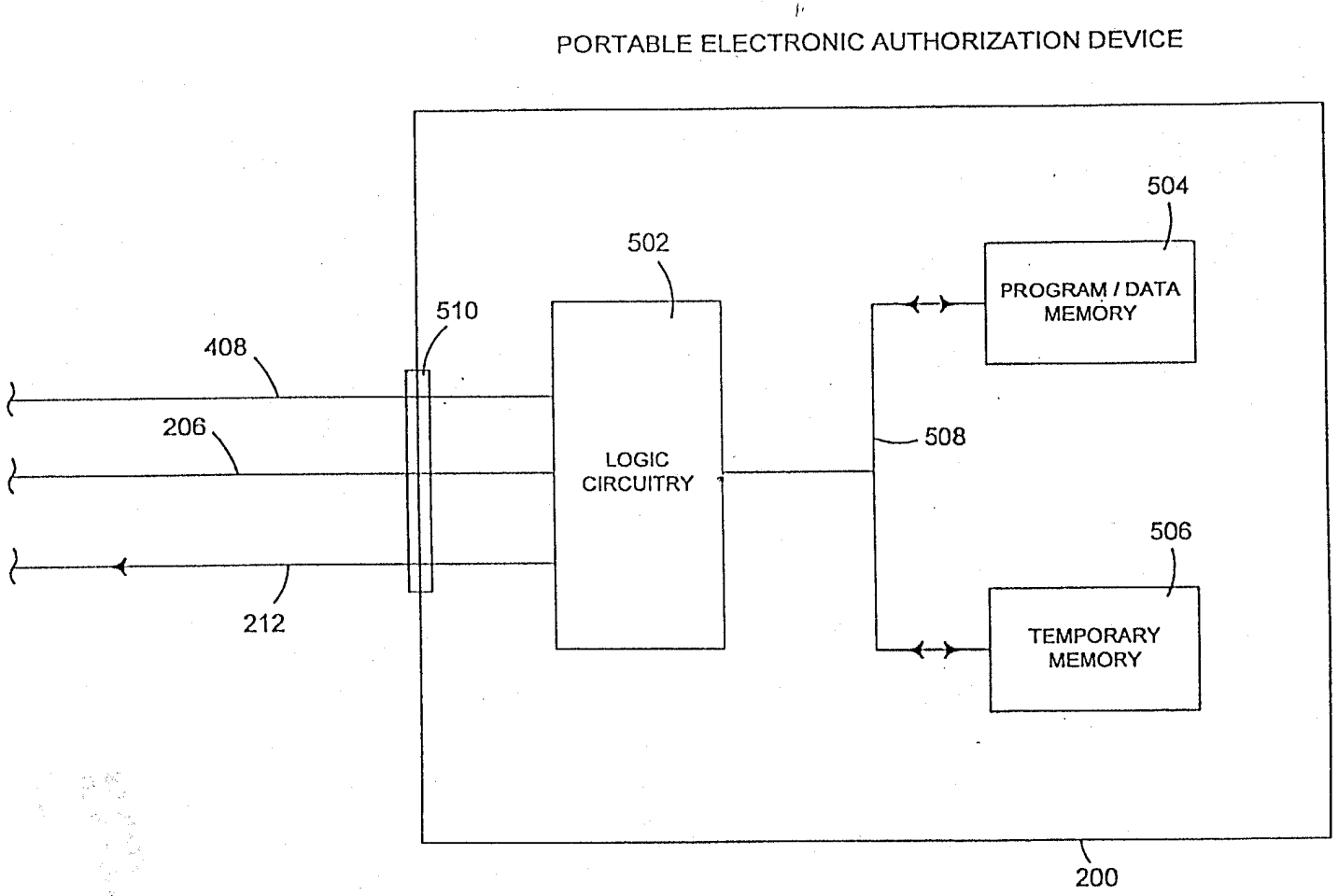

PORTABLE ELECTRONIC AUTHORIZATION DEVICE
504
502
510
PROGRAM / DATA MEMORY
408
206
LOGIC CIRCUITRY
508
506
TEMPORARY MEMORY
212
200

FIG. 5A

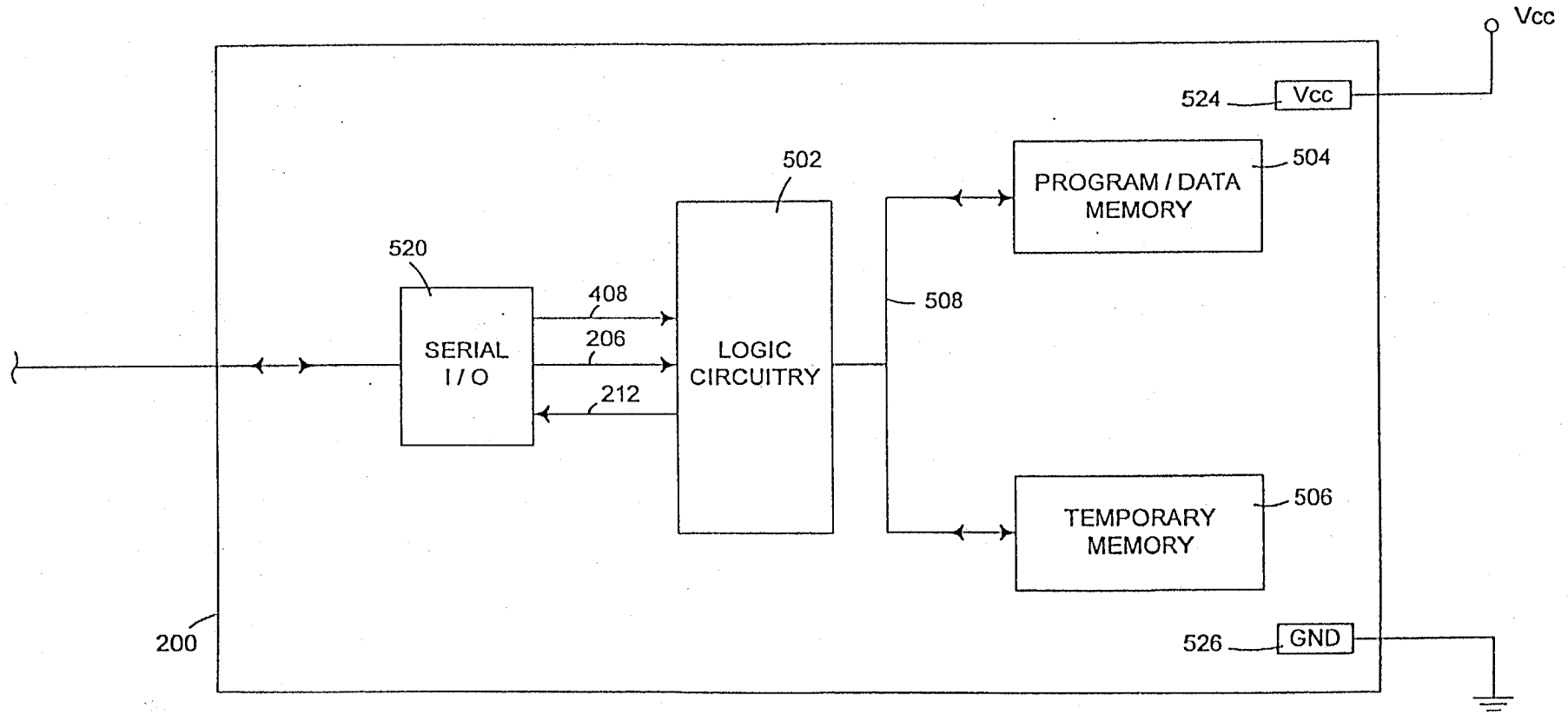

PORTABLE ELECTRONIC AUTORIZATION DEVICE
Vcc
524
Vcc
502
504
PROGRAM / DATA MEMORY
520
408
206
212
SERIAL I / O
LOGIC CIRCUITRY
508
506
TEMPORARY MEMORY
200
526
GND

FIG. 5B

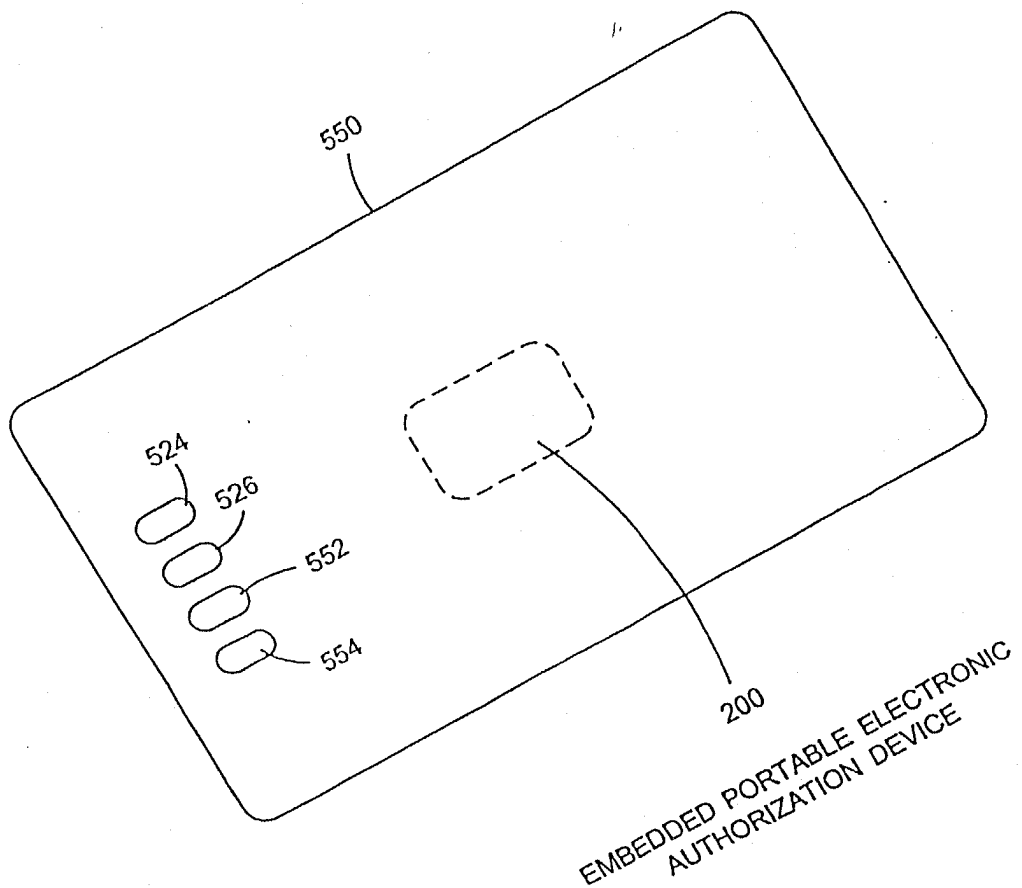

550
524
526
552
554
200
EMBEDDED PORTABLE ELECTRONIC AUTHORIZATION DEVICE

FIG. 5C

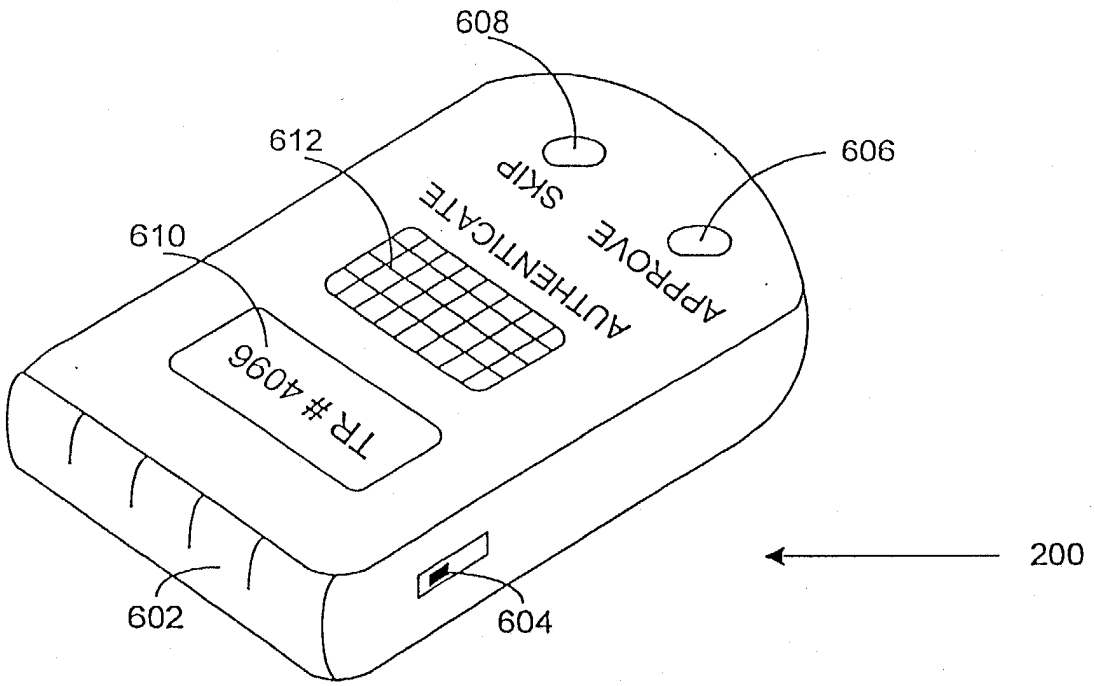

608
612
606
610
SKIP
APPROVE
AUTHENTICATE
TR # 4096
602
604
200

FIG. 6A

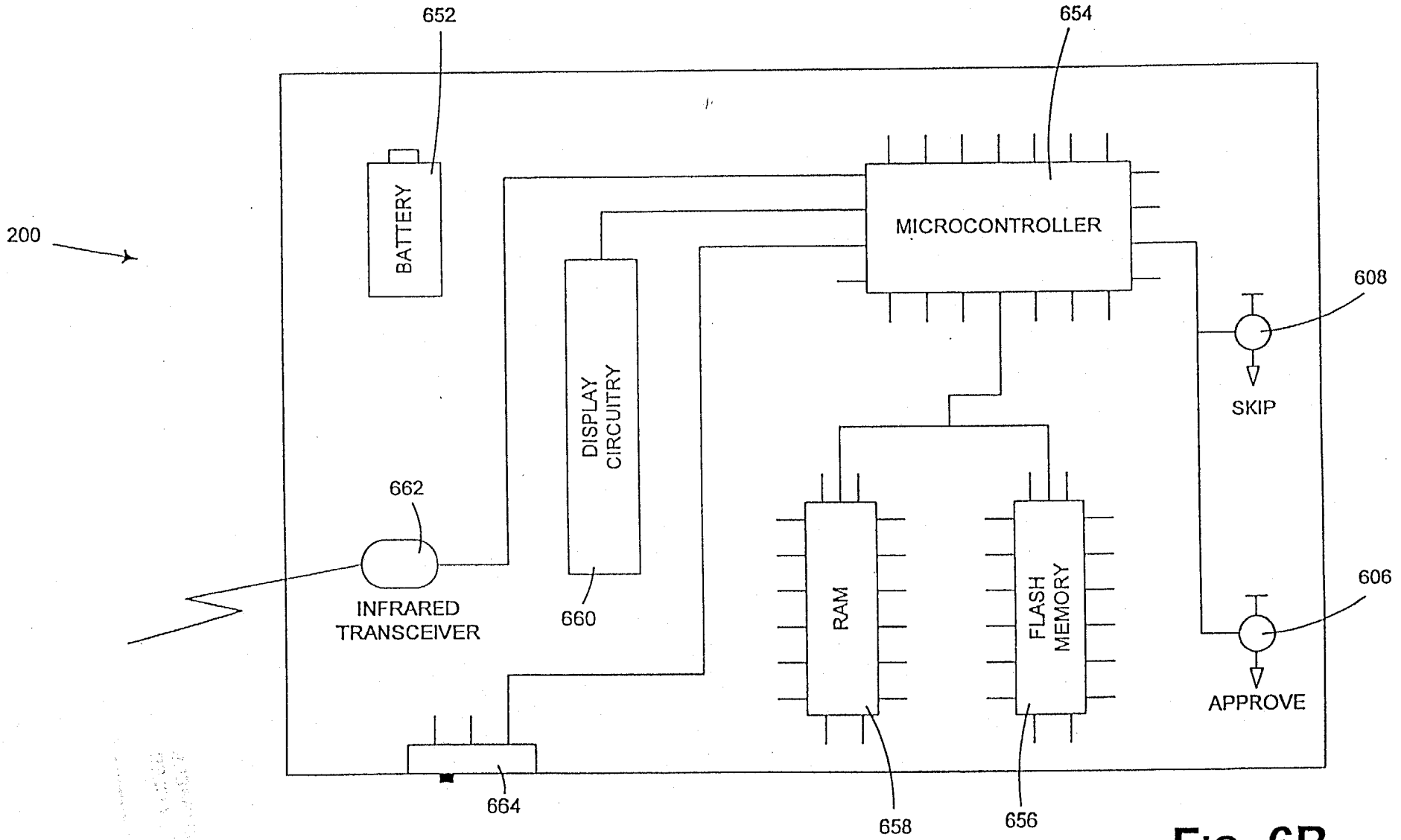

652
654
200
BATTERY
MICROCONTROLLER
608
SKIP
DISPLAY CIRCUITRY
662
INFRARED TRANSCEIVER
660
RAM
FLASH MEMORY
606
APPROVE
664
658
656

FIG. 6B

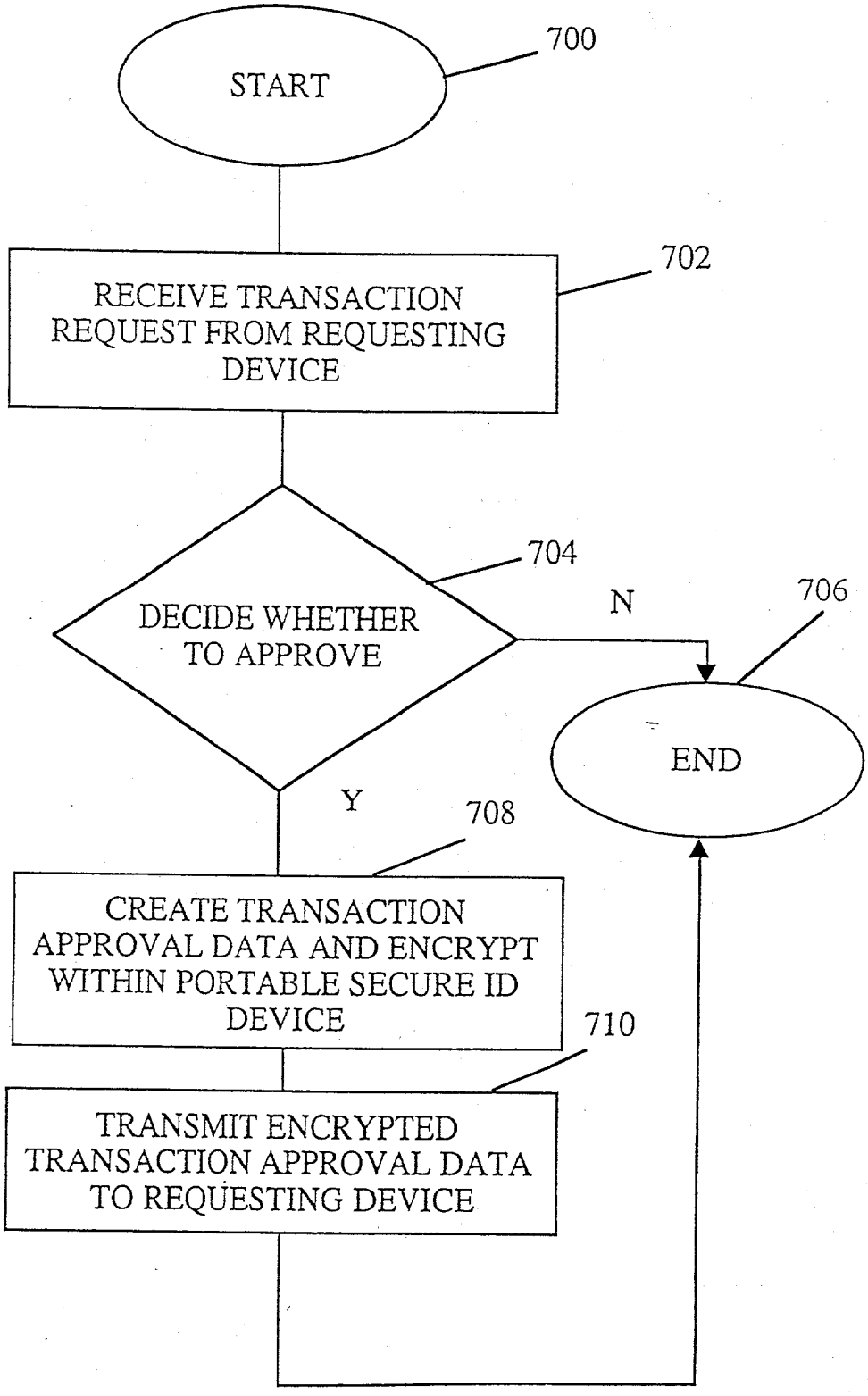

START
700
RECEIVE TRANSACTION REQUEST FROM REQUESTING DEVICE
702
DECIDE WHETHER TO APPROVE
704
N
706
END
Y
708
CREATE TRANSACTION APPROVAL DATA AND ENCRYPT WITHIN PORTABLE SECURE ID DEVICE
710
TRANSMIT ENCRYPTED TRANSACTION APPROVAL DATA TO REQUESTING DEVICE

FIG. 7

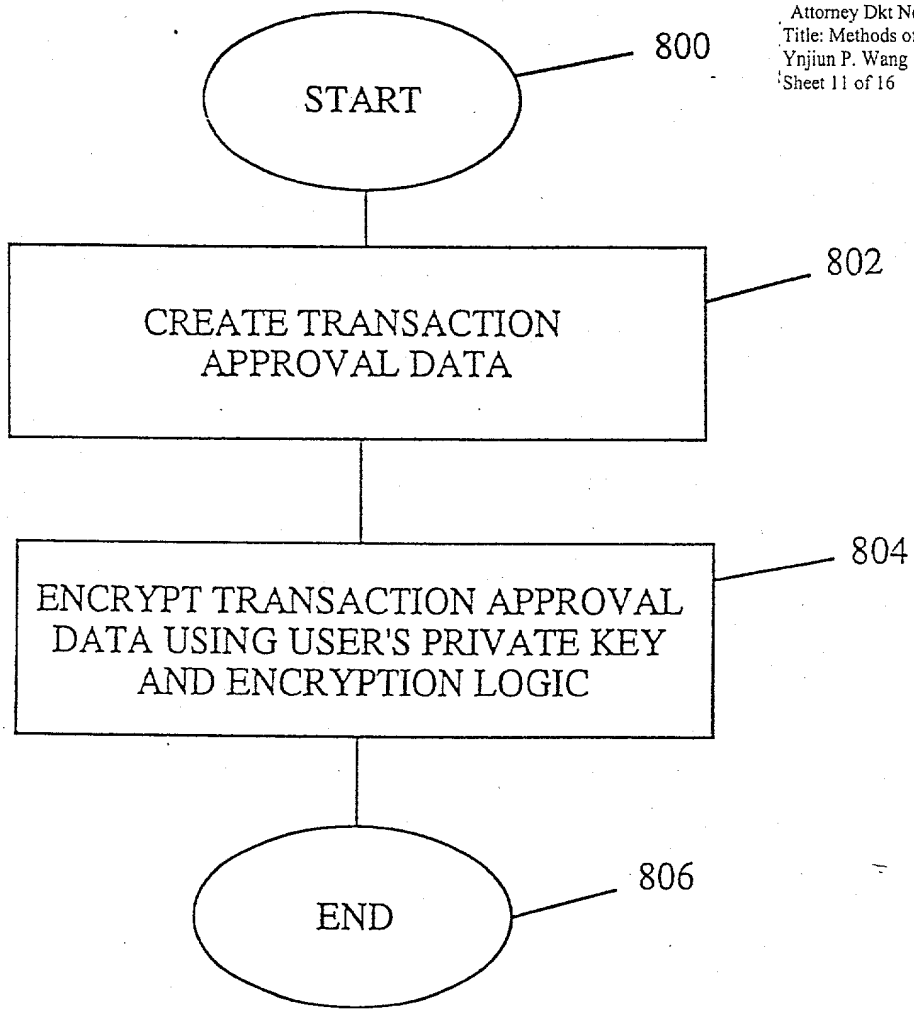

START
800
CREATE TRANSACTION APPROVAL DATA
802
ENCRYPT TRANSACTION APPROVAL DATA USING USER'S PRIVATE KEY AND ENCRYPTION LOGIC
804
END
806

FIG. 8

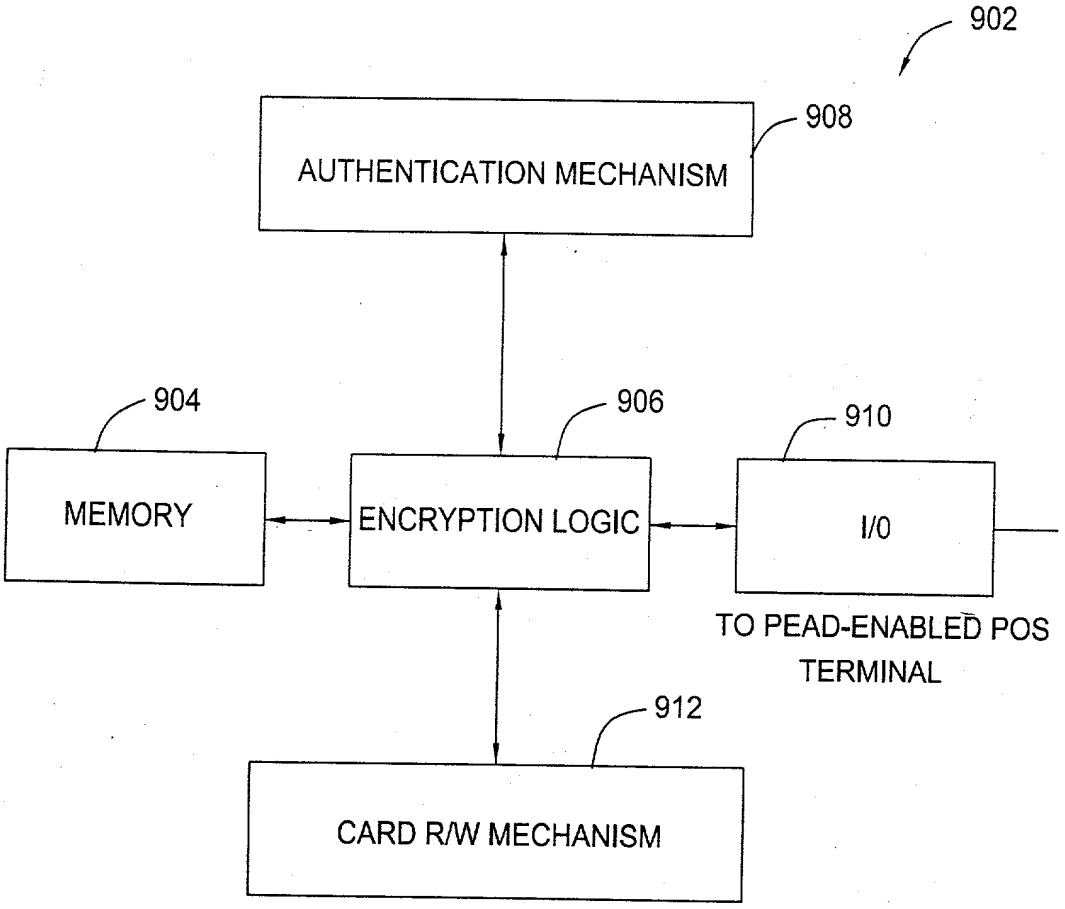

902
AUTHENTICATION MECHANISM
908
904
906
910
MEMORY
ENCRYPTION LOGIC
I/0
TO PEAD-ENABLED POS TERMINAL
912
CARD R/W MECHANISM

FIG. 9

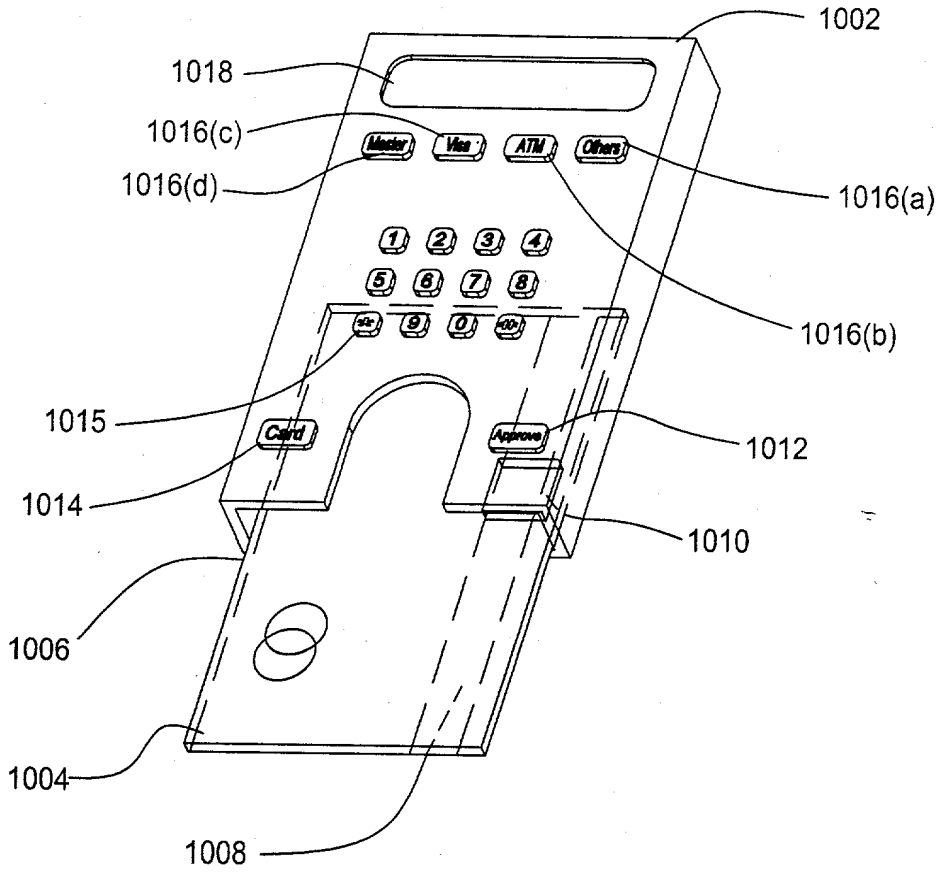

1002
1018
1016(c)
1016(d)
1016(a)
1016(b)
1015
1012
1014
1010
1006
1004
1008
Master
Visa
ATM
Others
Card
Approve

FIG. 10

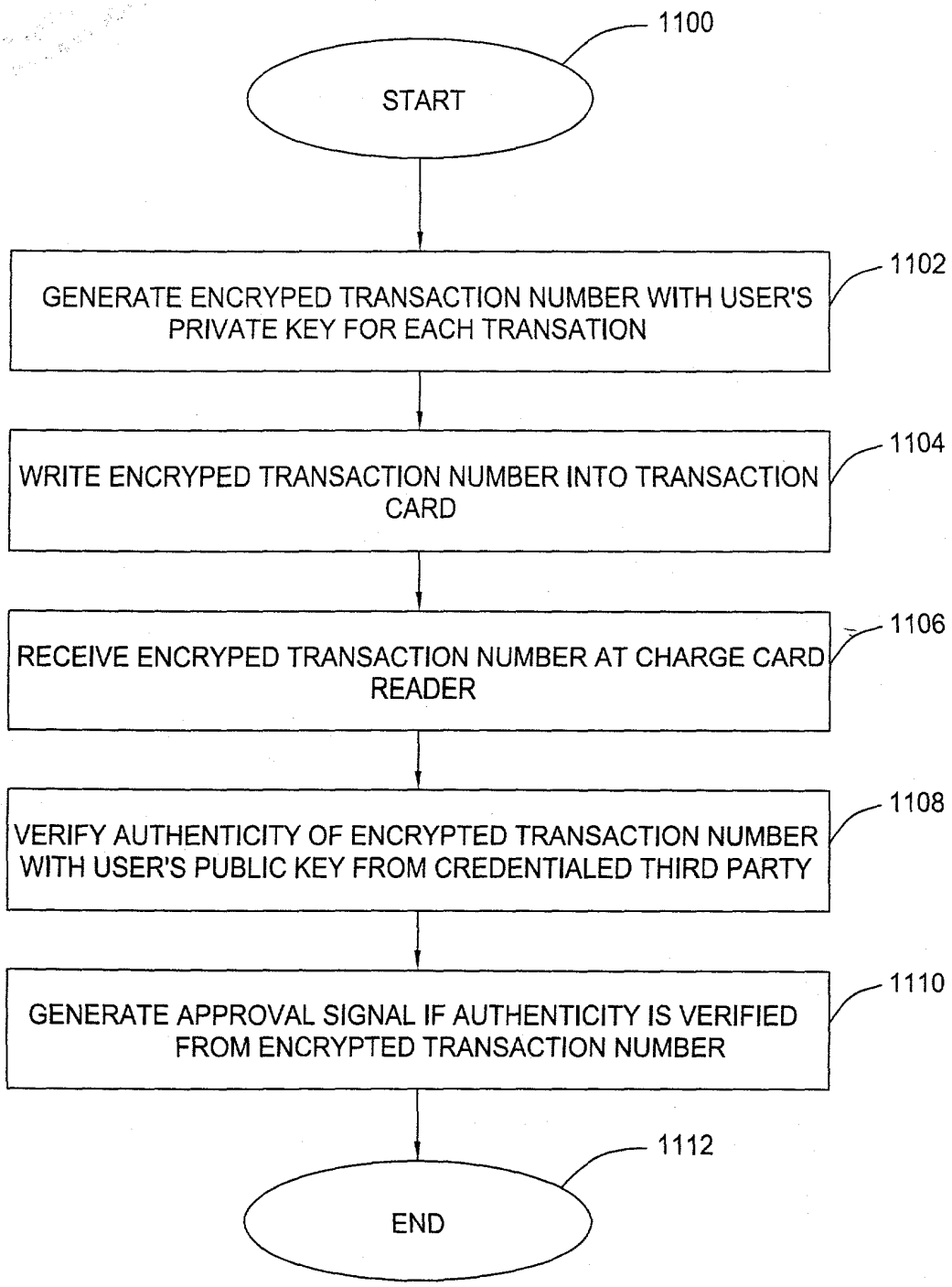

1100
START
GENERATE ENCRYPED TRANSACTION NUMBER WITH USER'S PRIVATE KEY FOR EACH TRANSATION
1102
WRITE ENCRYPED TRANSACTION NUMBER INTO TRANSACTION CARD
1104
RECEIVE ENCRYPED TRANSACTION NUMBER AT CHARGE CARD READER
1106
VERIFY AUTHENTICITY OF ENCRYPTED TRANSACTION NUMBER WITH USER'S PUBLIC KEY FROM CREDENTIALED THIRD PARTY
1108
GENERATE APPROVAL SIGNAL IF AUTHENTICITY IS VERIFIED FROM ENCRYPTED TRANSACTION NUMBER
1110
END
1112

FIG. 11

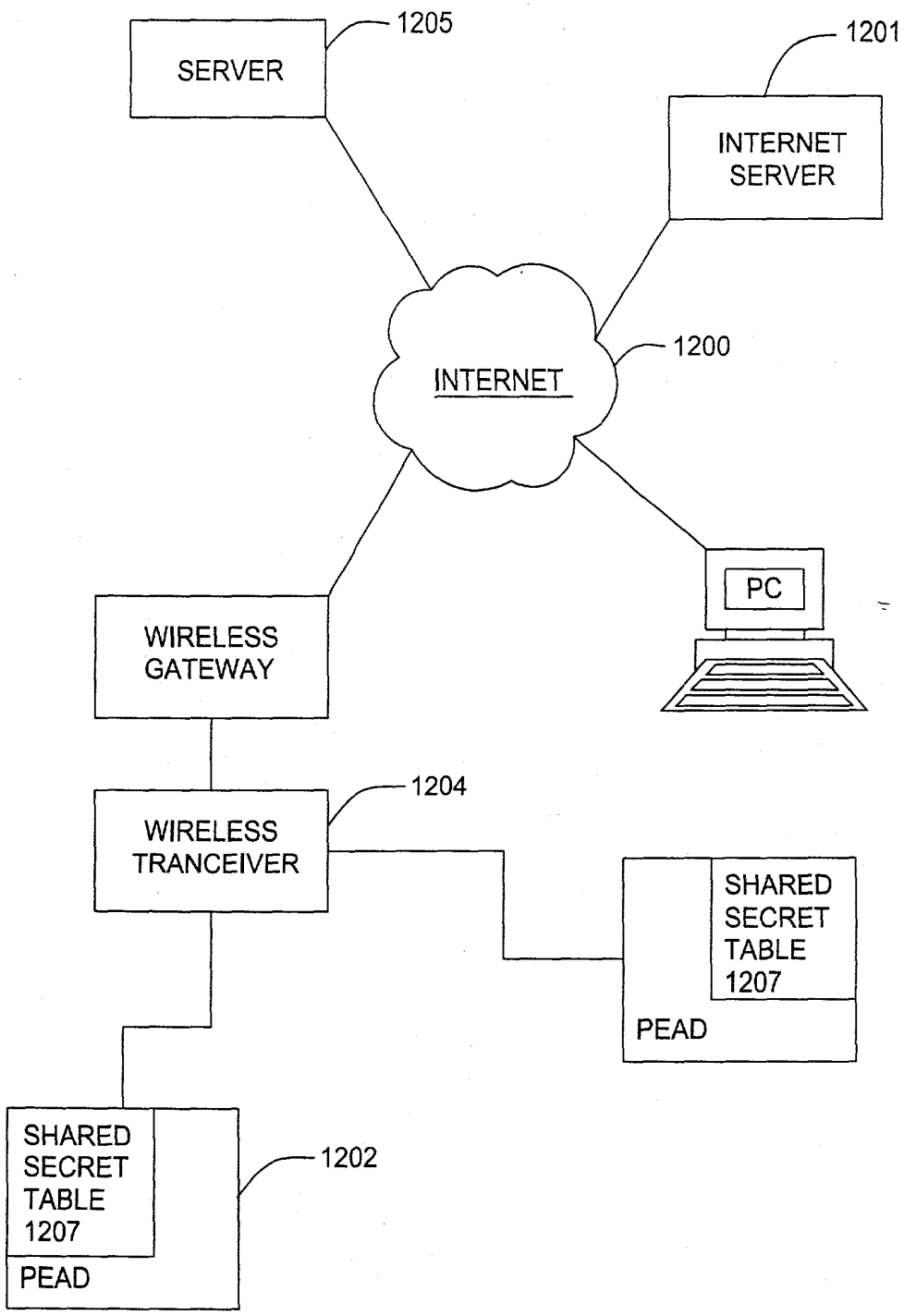

SERVER
1205
1201
INTERNET SERVER
INTERNET
1200
PC
WIRELESS GATEWAY
1204
WIRELESS TRANCEIVER
SHARED SECRET TABLE 1207
PEAD
SHARED SECRET TABLE 1207
PEAD
1202

FIG. 12A

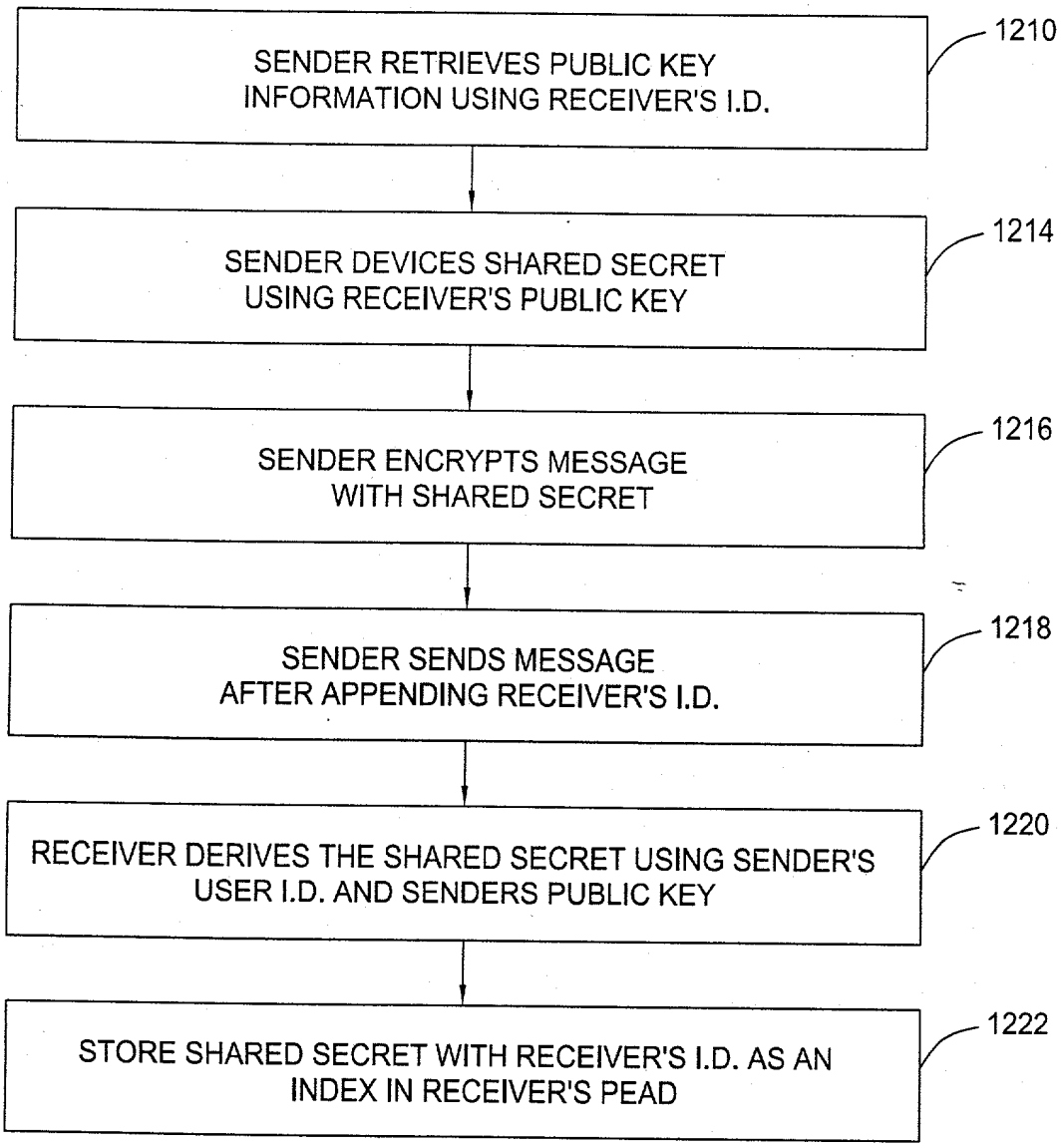

SENDER RETRIEVES PUBLIC KEY INFORMATION USING RECEIVER'S I.D.
1210
SENDER DEVICES SHARED SECRET USING RECEIVER'S PUBLIC KEY
1214
SENDER ENCRYPTS MESSAGE WITH SHARED SECRET
1216
SENDER SENDS MESSAGE AFTER APPENDING RECEIVER'S I.D.
1218
RECEIVER DERIVES THE SHARED SECRET USING SENDER'S USER I.D. AND SENDERS PUBLIC KEY
1220
STORE SHARED SECRET WITH RECEIVER'S I.D. AS AN INDEX IN RECEIVER'S PEAD
1222

FIG. 12B